Revue d'actualité de l'OSSIR

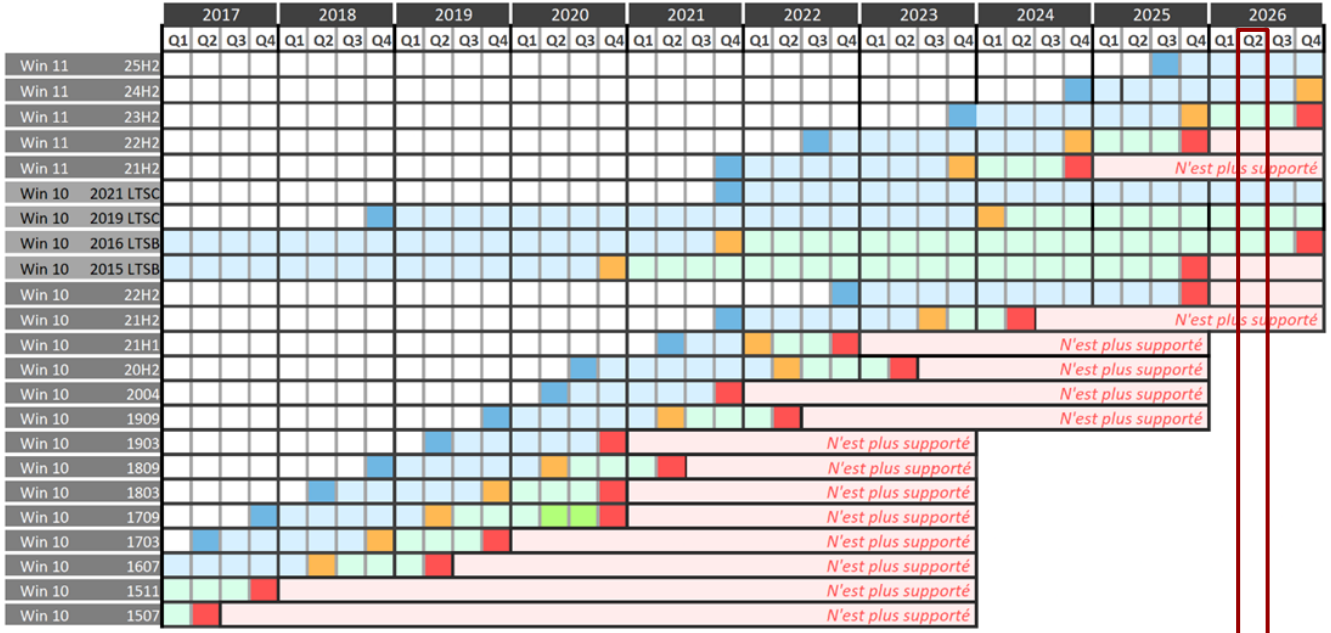
12 mai 2026

Jérémy De Cock
Melchior Courtois

<< La veille vous est fournie par cyberzen *>>*

Rappel du support Windows en couleurs

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Workstation***



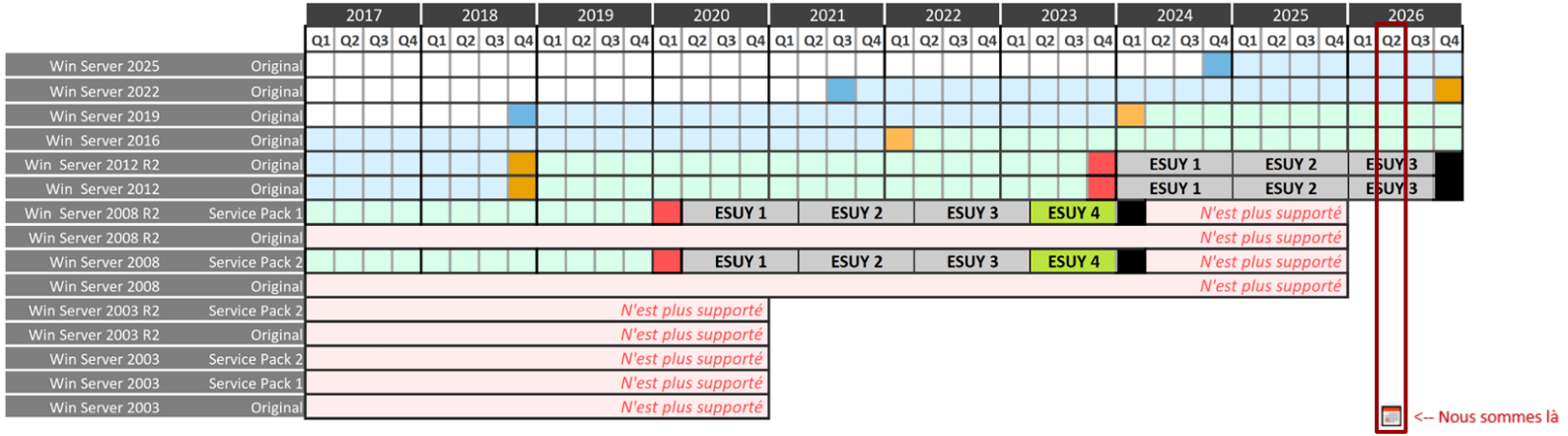
Sortie	Home, Pro	Entreprise
mardi 30 septembre 2025	mardi 12 octobre 2027	mardi 10 octobre 2028
mardi 1 octobre 2024	mardi 13 octobre 2026	mardi 12 octobre 2027
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 18 octobre 2022	mardi 14 octobre 2025	mardi 14 octobre 2025
mardi 16 novembre 2021	jeudi 13 juillet 2023	mardi 11 juin 2024
mardi 18 mai 2021	mardi 13 décembre 2022	mardi 13 décembre 2022
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 11 mai 2021
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
mercredi 5 avril 2017	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	mardi 9 mai 2017	mardi 9 mai 2017

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

LTSB : **L**ong-**T**erm **S**ervicing **B**ranch
LTSC : **L**ong-**T**erm **S**ervicing **C**hannel

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Server***



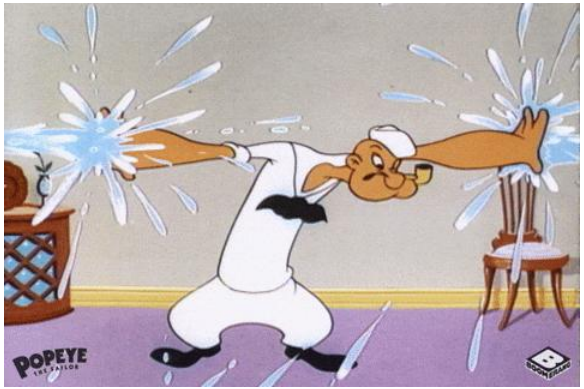
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 30 octobre 2012	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 22 février 2011	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
jeudi 22 octobre 2009	mardi 9 avril 2013		
mercredi 29 avril 2009	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
mardi 6 mai 2008	mardi 12 juillet 2011		
mardi 13 mars 2007	mardi 14 juillet 2015		
dimanche 5 mars 2006	mardi 14 avril 2009		
mardi 13 mars 2007	mardi 14 juillet 2015		
mercredi 30 mars 2005	mardi 14 avril 2009		
mercredi 28 mai 2003	mardi 10 avril 2007		

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour la version standard
- Support étendu pour LTSB/LTSC
- Fin de support étendu pour LTSB/LTSC
- X Extension d'une ou plusieurs années (ESUY)
- X Extension disponible uniquement avec Azure (Microsoft Entra ID)
- Fin de support pour la ou les extensions supplémentaires

ESYC : **E**xtended **S**ecurity **U**pdate **Y**ear

Failles / Bulletins / Advisories



Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin d'avril, 167 vulnérabilités patchées dont

- 2 vulnérabilités de type 0-day :
  - [**CVE-2026-32201**] Spoofing d'identité, Microsoft SharePoint Server
    - Validation incorrecte des données saisies
    - Ajoutée au catalogue KEV de la CISA
    - Affecte SharePoint Server Subscription Edition (SE), SharePoint Server 2019 et Enterprise Server 2016
  - [**CVE-2026-33825**] Elévation de privilèges, Microsoft Defender
    - Pas exploitée à l'heure actuelle mais le risque est réel
    - Corrigée par l'intermédiaire d'une MAJ sur sa plateforme Antimalware (v4.18.26030.3011)
- Les plus critiques :
  - [**CVE-2026-23666**] RCE, .NET Framework
  - [**CVE-2026-32190**] Déni de service, Microsoft Office
  - [**CVE-2026-33115,33114**] RCE, Microsoft Office - Word
  - [**CVE-2026-32157**] RCE, Client Bureau à distance de Windows
  - [**CVE-2026-33826**] RCE, Active Directory
  - [**CVE-2026-33824**] RCE, Extension IKE de Windows
  - [**CVE-2026-33827**] RCE, Pile TCP/IP de Windows

https://www.it-connect.fr/patch-tuesday-avril-2026-recapitulatif-microsoft/

Failles / Bulletins / Advisories
Système

C’est si simple de devenir root sur Linux #CopyFail


CVE-2026-31431

- Elévation de privilèges en local
  - Vulnérabilité trouvée par Xint Code
  - API `AF_ALG` + `splice()` = écriture de 4 octets dans le page cache de n’importe quel fichier
    - Imaginons dans */usr/bin/su* ? 💥
- Introduit en 2017 lors de l’optimisation de *algif_aead.c*
- Aucune différence entre les distributions
- Solutions ?
  - Patchez (annulation de l’optimisation de 2017)
  - Ou désactivez le module `algif_aead` au niveau du noyau :

```
echo "install algif_aead /bin/false" > /etc/modprobe.d/disable-algif.conf
rmmod algif_aead 2>/dev/null || true
```

https://korben.info/copy-fail-faille-kernel-linux-decouverte-ia.html

https://www.linkedin.com/posts/fredraynal_3-d%C3%A9veloppeurs-3-commits-9-ans-de-root-activity-7456609226723946496-hJHr/

Failles / Bulletins / Advisories
Système

Si si… vraiment #DirtyFrag


CVE-2026-31431

- Elévation de privilèges en local
  - Des similitudes avec CopyFail et Dirty Pipe
  - Vulnérabilité déclenchée lors d'une opération cryptographique « sur place »
  - Permet d'écraser directement des données en RAM → modification à la volée de fichiers critiques
    - Imaginons dans */usr/bin/su* ? 💥
- Deux vulnérabilités permettant l'écriture arbitraire de plusieurs octets
  - `xfrm-ESP` : privilèges pour créer un namespace nécessaires
  - `RxRPC` : nécessite le module noyau `rxrpc.ko`
- Aucune différence entre les distributions
- Solutions ?
  - Patchez
  - Ou supprimez les modules concernés :

```
sh -c "printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc
/bin/false\n' > /etc/modprobe.d/dirtyfrag.conf
rmmod esp4 esp6 rxrpc 2>/dev/null; true"
```

https://www.it-connect.fr/dirty-frag-cette-faille-zero-day-donne-les-droits-root-sur-linux/

https://www.linkedin.com/posts/fredraynal_jai-d%C3%A9cortiqu%C3%A9-copy-fail-cve-2026-31431-activity-7457811766102802432-7v0i/

Failles / Bulletins / Advisories
Système

Multiples failles dans Apache

CVE-2026-23918

- Patch disponible corrigeant de nombreuses failles
  - RCE critique sur la version v2.4.66
    - Bug lors de l'envoie d'une trame `HTTP/2 HEADERS` immédiatement suivie d'une trame `RST_STREAM` sur le même flux
    - Cela crée une opération en double dans le tableau de nettoyage, donc le système tente de détruire une zone mémoire qui a déjà été libérée
    - Peut entraîner un DoS ou une RCE
- Montée de version recommandée → v2.4.67

https://www.it-connect.fr/faille-apache-deux-simples-trames-suffisent-a-faire-un-deni-de-service-cve-2026-23918/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

0-day sur Adobe Reader


CVE-2026-34621

- Premier échantillon déposé sur VirusTotal le 28 novembre
  - Sous le nom de *Facture540.pdf*
  - Fortement exploitée depuis décembre 2025
- Déclenche automatiquement l'exécution de JavaScript obscurci
  - Récolte des données sensibles et réception de charges utiles supplémentaires
- Patch disponible
  - Version v4.0.0

https://thehackernews.com/2026/04/adobe-reader-zero-day-exploited-via.html

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

Wordpress, plugin Slider Revolution vulnérable


CVE-2026-6692

- + 5M de téléchargements du plugin
- Faille signalée le 18 avril
  - Permet le téléchargement de fichiers arbitraires → RCE possible
    - Manque de validation des extensions de fichiers lors de l'utilisation de certaines fonctions du plugin, notamment la fonction `_check_file_path`
    - Possible de fournir une URL pointant vers un fichier PHP malveillant
- Versions affectées : 7.0.0 à 7.0.10
  - Patcher dans la version v7.0.11

https://www.it-connect.fr/wordpress-le-plugin-slider-revolution-doit-etre-mis-a-jour-cve-2026-6692/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Age Verification, piratée en… 2 minutes

- Permet aux européens de prouver qu'ils ont l'âge requis pour accéder aux réseaux sociaux
  - Obligation qui doit entrer en vigueur en septembre prochain
  - « L'application est totalement **anonyme**, elle **fonctionne sur n'importe quel appareil** et son logiciel est entièrement **open source**, ce qui signifie que les pays partenaires dans le monde entier peuvent également l'adopter. »
- Une vulnérabilité dans la gestion du code PIN ?
  - Besoin de créer un code PIN lors de la première utilisation de l'application
    - Permet de déverrouiller l'accès à ses informations et de prouver son âge
  - Résulat(s) ?
    - Le code PIN est chiffré localement = possibilité de définir un nouveau code PIN en supprimant certaines valeurs
    - Limitation du nombre de codes PIN saisis réalisé via un compteur stocké dans un fichier. On le passe à 0 ?
    - Biométrie contrôlé via un paramètre booléen. On le passe à false ?
- Cela fait réagir Pavel Durov (Telegram) : « outil de surveillance vendu comme respectueux de la vie privée »

https://x.com/paul_reviews/status/2044723123287666921

Piratages, Malwares, spam, fraudes et DDoS
Piratage

CloudZ RAT, malware Smartphone/Windows

- Piratage lié à l'application Mobile Connecté de Windows
  - Permet d'intercepter les SMS et les mots de passe à usage unique (OTP)
- Compromission initial liée à un fichier malveillant se faisant passer pour une mise à jour de l'outil ScreenConnect
  - Communication vers les serveurs C2 pour compromission total
- Recommandation : éviter d'utiliser l'application Mobile Connecté

https://www.it-connect.fr/cloudz-rat-ce-malware-espionne-vos-sms-via-lapplication-mobile-connecte-de-windows/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Malwares signés à l'aide de certificats volés

- Intrusion sur les systèmes internes de DigiCert
  - Réalisée via de l'ingénierie sociale : client fake auprès du support technique
    - Accès possible pendant 2 semaines
  - Données volées permettant d'émettre des certificats EV de signature de code
- Quelques chiffres :
  - 60 certificats émis pendant la période d'exposition ont été révoqués par mesure de sécurité
  - 27 certificats étaient directement liés à l'activité de l'attaquant
  - 11 d'entre eux avaient déjà été signalés par des chercheurs en sécurité
    - Ayant été utilisés dans des campagnes malveillantes
- Certificats utilisés pour signer des payloads du malware Zhong Stealer
  - Infostealer et cryptostealer
- GoldenEyeDog 🇨🇳 à l'origine de cette intrusion ?

https://www.it-connect.fr/piratage-digicert-des-malwares-signes-a-laide-de-certificats-voles/

Piratages, Malwares, spam, fraudes et DDoS
Ransomware

Services municipaux bloqués à Quiberon

- Attaque subie le 3 mai et rendue publique 2 jours plus tard
  - Revendiquée par le groupe Quilin
- La mairie assure que les services locaux restent accessibles (aux heures habituelles)
  - Et sans les outils informatiques

https://www.it-connect.fr/la-ville-de-quiberon-nouvelle-victime-du-ransomware-qilin/

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

Données des magasins U en ligne

- Piratage de l'enseigne et vol de données personnelles
  - Civilité, statut client professionnel, noms, prénoms, mails, adresses postales, numéros de téléphone et numéros de carte de fidélité
  - PAS de coordonnées bancaires selon l'enseigne
- Déclaration CNIL et alerte client
  - Recommandation de modifier son mot de passe de compte et le code PIN de la carte du magasin

https://www.01net.com/actualites/les-magasins-u-ont-ete-pirates-les-donnees-des-clients-ont-ete-compromises.html

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

5 mois trop tard, la cyberattaque de Parcoursup

- Piratage de Parcoursup en automne 2025
  - Exfiltration des données (705.000 personnes)
- Utilisation des credentials d'un agent de la région Occitanie
- Différents types de données volées :
  - Noms, prénoms, dates de naissance et nationalités des victimes, adresses postales, adresses e-mail et numéros de téléphone
  - Filière suivie, formation envisagée et statut de boursier
  - Informations sur leurs parents ou tuteurs légaux pour les mineures

https://www.01net.com/actualites/fuite-donnees-parcoursup-cyberattaque-passee-inapercue-pendant-six-mois.html

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

Accès sur la plateforme EduConnect

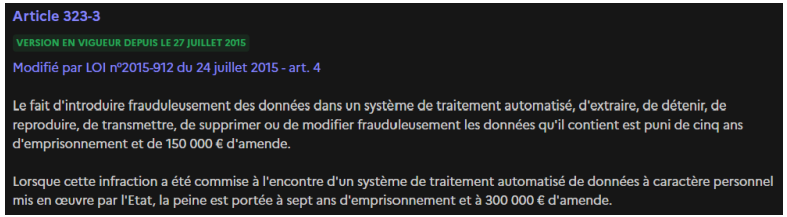
- Intrusion revendiquée par Dumpsec
  - Accès sur la plateforme possible via l'usurpation d'un compte interne
    - + exploitation d'une faille corrigée fin 2025 ?
- Données concernées :
  - Noms, prénoms, identifiants, établissements / classes, adresses mails (si renseignée) et codes

https://www.it-connect.fr/piratage-educonnect-les-donnees-personnelles-deleves-dans-la-nature/

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

18 millions de Français impactés par le piratage ANTS

- Cyberattaque ayant eu lieu le 15 avril 2026
- Données concernées :
  - Identifiants de connexion, civilité, noms, prénoms, adresses mails, dates de naissance, identifiants uniques des comptes, adresses postales, lieux de naissance et téléphone
- Les pièces jointes transmises via le portail ANTS sont épargnées
- Un jeune de 15 ans derrière tout ça ?
  - Placé en garde à vue le 25 avril
  - Relié à une centaine de signalements de piratages
    - Depuis le 19 décembre !



https://www.it-connect.fr/piratage-ants-18-millions-de-francais-potentiellement-impactes-par-une-fuite-de-donnees/

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

Udemy, victime du groupe ShinyHunters

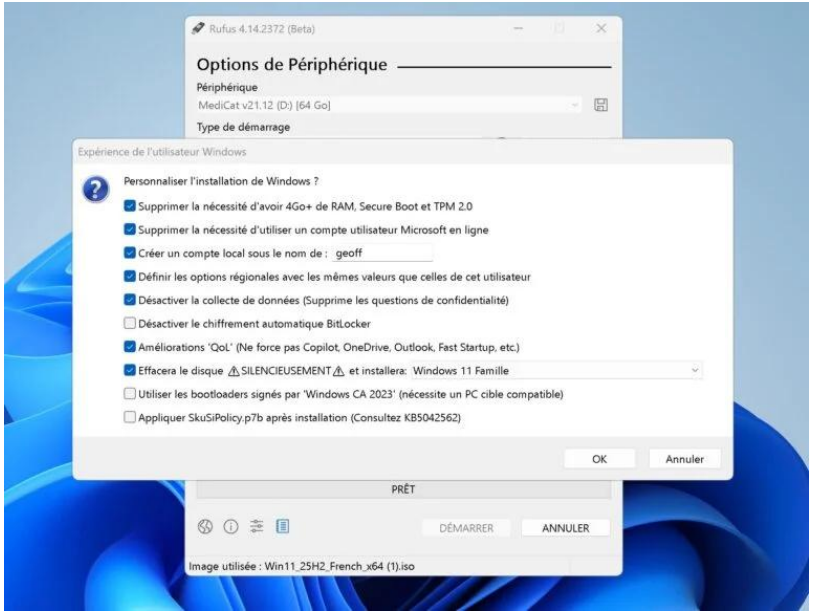
- Publication d'une base de données concernant + 1.4 million d'enregistrements
  - Noms, prénoms, adresses postales, numéros de téléphone, informations sur les postes et sur les employeurs et méthodes de paiement
- Base de données ajoutée sur la plateforme Have I Been Pwned
- Aucune communication de la part d'Udemy

https://www.it-connect.fr/cyberattaque-udemy-le-gang-shinyhunters-publie-les-donnees-1-4-million-utilisateurs/

Piratages, Malwares, spam, fraudes et DDoS
Technique & outil

MAJ Rufus très pratique

- Mise à jour de l'outil avec 2 nouvelles fonctionnalités
  - Amélioration QoL (Quality of Life)
  - Installation silencieuse
    - Plus besoin d'être devant l'écran



https://www.01net.com/actualites/windows-11-rufus-profite-dune-importante-mise-a-jour-qui-lui-offre-de-nouveaux-pouvoirs.html

Piratages, Malwares, spam, fraudes et DDoS
Technique & outil

Explainshell : le traducteur de commande

- Outil web permet de comprendre les commandes du terminal (GNU/Linux)
  - Décompose la commande étape par étape
  - Affiche une explication claire pour chaque élément
- Pratique pour comprendre des commandes inconnues ou longues

https://explainshell.com/

Piratages, Malwares, spam, fraudes et DDoS
Publication

Guide stratégique de l'IA

- Intitulé « The AI Vulnerability Storm: Building a Mythos-ready Security Program »
  - Brief stratégique publié en avril 2026
  - Par la Cloud Security Alliance, avec le SANS Institute et le projet OWASP GenAI Security Project
  - Destiné principalement aux CISOs (RSSI)
- En bref, l'explosion de l'utilisation de l'IA pour la détection des failles devient difficile à corriger
  - Surcharge des équipes de sécurité
  - Déploiement de correctifs lent et complexe
- Plusieurs remediations existent, cependant :
  - Renforcer les bases (segmentation réseau, MFA, filtrage des flux sortants, défense en profondeur)
  - Utiliser l'IA à son tour (test de sécurité, détection)

https://labs.cloudsecurityalliance.org/wp-content/uploads/2026/04/mythosreadyv9.pdf

Business et Politique

Business
Monde

Claude prends des libertés sur navigateurs

- Modification par l'IA des permissions sur les navigateurs
  - Application peut donc agir sur le navigateur avec les droits de l'utilisateur
    - Lire vos pages
    - Remplir vos formulaires
    - Capturer l'écran sur des sessions authentifiées
    - Valider des actions
- Aucun commentaire de Anthropic sur ce comportement
  - Premisse pour Computer Use
    - Fonctionnalité permettant à Claude d'utiliser votre PC comme un humain

https://korben.info/claude-desktop-modifie-les-permissions-de-navigateurs-que-vous-navez-meme-pas-installes.html

Business
National

Airbus s’offre Quarkslab

- Quarkslab rejoint l’unité « Connected Intelligence » de ADS
  - *« L'expertise profonde de Quarkslab et de ses équipes vient renforcer un acteur cyber résilient et souverain en France et en Europe. Cette acquisition renforcera notre capacité à construire le bouclier numérique nécessaire pour maintenir nos nations et nos alliés en tête dans le domaine de la cybersécurité »* #François Lombard, Head of Connected Intelligence chez Airbus Defence and Space
- Un gros intérêt pour la solution QShield
  - Permet de protéger le code source et les secrets industriels contre le reverse engineering

https://www.zdnet.fr/actualites/airbus-soffre-quarkslab-la-souverainete-cyber-francaise-change-de-dimension-494108.htm

Droit / Juridique / Politique
Europe

PDS : transition de Microsoft vers Scaleway !

- Contrat associé au Health Data Hub décroché par la filiale Cloud du groupe Iliad
  - Les données de santé des Français seront donc hébergées sur des infrastructures souveraines !
- Processus de sélection qui aura été long : 2 mois et demi
  - 350 exigences techniques à respecter
  - La qualification SNC doit être obtenue → condition non négociable
- Migration attendue entre fin 2026 et début 2027
- Raisons de cette transition ?
  - Souveraineté des données
  - Risque juridique liée au CLOUD Act et au FISA
  - Qualification SecNumCloud

https://www.health-data-hub.fr/actualites/la-plateforme-des-donnees-de-sante-engage-sa-migration-vers-un-cloud-souverain-avec

Droit / Juridique / Politique
National

Bye Windows, welcome Linux

- DINUM : Volonté de transition vers une infrastructure souveraine
  - 1ère migration avec 250 agents (250 ordinateurs)
  - Utilisation d'outils spécifiques pour le quotidien avec LaSuite
    - Visio
    - Tchap
    - France Transfert
- Rappel : plan de transition pour automne 2026 pour TOUS les ministères

  https://www.it-connect.fr/la-dinum-passe-de-windows-a-linux-les-autres-ministeres-doivent-preparer-leur-plan/

Opérations internationales

Opérations internationales
Opération

Phishing KO

- Démantèlement d'un réseau de phishing par le FBI
  - Connu sous le nom de W3LL
  - Plus de 17.000 victimes grâce aux outils proposés
  - Plus de 20M$ extorqués
- Opération en collaboration avec la police indonésienne

https://techcrunch.com/2026/04/13/fbi-announces-takedown-of-phishing-operation-that-targeted-thousands-of-victims/

Conférences

Conférences

Passée(s)

- sambaXP, 20 au 21 avril en ligne
- Botconf, 15 au 17 avril à Reims

À venir

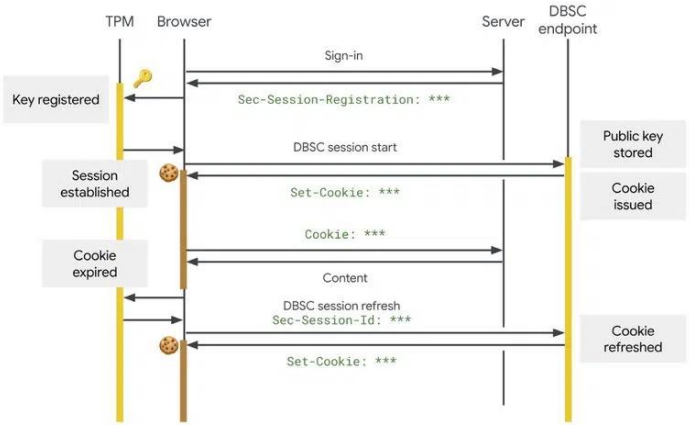
- Cyber On Board, 26 au 28 mai sur la Presqu'île de Giens
- ESIEA Secure Edition, 30 mai à Ivry-sur-Seine
- SSTIC, 3 au 5 juin à Rennes
- LeHACK, 26 au 28 juin à Paris
- Pass the SALT, 30 juin au 2 juillet à Lille

Divers / Trolls velus

Divers / Trolls velus

Nouvelle fonctionnalité dans Chrome 146 : DBSC

- DBSC (Device Bound Session Credentials)
  - Disponible uniquement sur Chrome pour Windows
  - S'appuie sur la puce TPM du PC
- Fonctionnement :
  - Génération de clés publiques à l'aide de la puce TPM
  - Stockage de la clé privée dans la puce TPM
  - Une session = une paire de clés
- Le service web en face doit implémenter DBSC
  - Un nouveau standard ?
    - Projet soumis au W3C
    - Développé avec Microsoft
  - La fin du vol de session ?



https://blog.google/security/protecting-cookies-with-device-bound-session-credentials/

Divers / Trolls velus

Microsoft Edge stocke les mots de passe en clair

- Spécialement les mots de passe du gestionnaire de mot de passe intégré
  - Les mots de passe sont stockés en mémoire à l'ouverture du navigateur…
  - …même si non sollicités
- Valable uniquement pour Microsoft Edge
- PoC disponible sur Github
  - Tool permettant de récupérer les informations du navigateur

https://www.it-connect.fr/un-chercheur-prouve-que-microsoft-edge-laisse-fuiter-vos-mots-de-passe-en-memoire/

FIN

Prochaine réunion ?

- RDV le **mardi 9 juin 2026**

Accéder aux différents supports ?

Replays

Slides

https://www.youtube.com/@OSSIR

https://www.ossir.org/support-des-presentations/